UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/806,172	07/13/2001	Jong Woo Lee	B-4151PCT 61	5202

36716 7590 09/10/2004

LADAS & PARRY
5670 WILSHIRE BOULEVARD, SUITE 2100
LOS ANGELES, CA 90036-5679

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	**PAPER NUMBER**
2135	9

DATE MAILED: 09/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/806,172	**Applicant(s)** LEE, JONG WOO	
	Examiner Paula W Klimach	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 June 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☑ All b)□ Some * c)□ None of:

1.☑ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 7.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

Claims 1 and 8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "the input" in line 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 8 recites the limitations:

“the keyboard," and “the computer” in line 2.

“the secure adapter," in line 3.

“the main processor," and “the secure code” in line 4.

“the keyboard," in line 5.

There is insufficient antecedent basis for this limitation in the claim.

The above examples are illustrative only. Applicant is requested to ensure that any other instances are corrected.

Claim Objections

Claim 8 is objected to because of the following informalities:

“secrete,” should be secret in line 3.

Appropriate correction is required.

The above examples are illustrative only. Applicant is requested to ensure that any other instances are corrected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1 and 7 are rejected under 35 U.S.C. 102(e) as being anticipated by Boebert (5,822,435).

Boebert discloses a method and apparatus for ensuring secure communication over unsecured communication medium. The apparatus transfers key code input from a keyboard to a computer system (Fig. 2), characterized in a configuration to transfer input from the keyboard to the computer system after encryption (column 8 lines 39-44) if a secure mode setup command is received from the keyboard or the computer system (column 5 line 66 to column 6 line 5), and to transfer the input from the keyboard to the computer system without encryption if a secure mode clearing command is received or under cleared secure mode (column 8 lines 35-38).

In reference to claim 7, where a separate secure key for entering secure mode setup/clearing command is incorporated in said keyboard and/or the secure mode setup/clearing command can be created by the combination of existing key codes, the computer system has the secure key creation function, the encryption/decoding function with the secrete key and the encryption/decoding function with the secure key, and the keyboard manager with application program interface is included (column 5 line 66 to column 6 line 5).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-4, 8-11, and 15-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boebert in view of Stallings.

In reference to claim 8, Boebert discloses a method and apparatus for ensuring secure communication over unsecured communication medium. When the apparatus is under secure mode, the main processor transfers the information to the stream cipher if the key code input information of the keyboard is transferred to the main processor through the transmit/receive control on the, keyboard, the stream cipher's encrypting the key code input information with the secret key and transferring the encrypted information to the keyboard manager through computer connection by the transmit/receive control on the computer; computer system decoding the encrypted information using the secret key (column 8 lines 39-44); main processor transferring the secure made clearing command to the stream cipher when the secure mode clearing command is transferred from the keyboard or the computer system to the main processor of the secure adapter (column 5 line 66 to column 6 line 5); and when secure mode is cleared, the stream cipher transferred key code input information to the keyboard manager through the computer connection by the transmit/receive control on the computer without encryption, if the key code input information of the keyboard is transferred to the stream cipher through the transmit/receive control on the keyboard after passing through the keyboard connection (Fig. 2 in combination with column 8 lines 35-38).

However Boebert does not disclose the key distribution and therefore transferring a secure key created in the keyboard manager of the computer system to the secure adapter in computer booting; creating a new secret key in the main processor when the secure mode setup command from the keyboard or the computer system is transferred to the main processor of the secure adapter, and then transferring the secrete key to the initial cipher and the stream cipher of the secure adapter; encrypting the secrete key with the secure key in the initial cipher and then transferring the encrypted secrete key to the keyboard manager through the computer connection by the transmit/receive control on the computer.

Stallings disclose decentralized key distribution wherein transferring a secure key (Master key) to the Responder B. The Responder B creates a new secret key (session key) and uses the Master key to encrypt the session key and send it to the Initiator A (Page 147).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the key distribution as disclosed by Stallings between the cryptographic entity and the workstation of Boebert. One of ordinary skill in the art would have been motivated to do this because it would be a safe method of transferring a new session key whenever key codes need to be encrypted.

In reference to claims 2, Boebert does not disclose a system further comprising: a main processor to process the secure mode setup/clear command and to create a secrete key in setting secure mode; an initial cipher to encrypt the secrete key transferred from the main processor with the secure key from the computer system and then to transfer the encrypted secrete key to the computer system; and a stream cipher to encrypt the key code input information from the keyboard with the secrete key and then to transfer the encrypted information to the computer

Stallings disclose decentralized key distribution wherein transferring a secure key (Master key) to the Responder B. The Responder B creates a new secret key (session key) and uses the Master key to encrypt the session key and send it to the Initiator A (Page 147).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the key distribution as disclosed by Stallings between the cryptographic entity and the workstation of Boebert. One of ordinary skill in the art would have been motivated to do this because it would be a safe method of transferring a new session key whenever key codes need to be encrypted.

In reference to claim 3, Boebert discloses a method and apparatus further comprising: a computer connection coupled to a keyboard port of the computer (Fig. 3 part 46); a keyboard connection coupled to a keyboard plug (Fig 3 part 20); a transmit/receive control on the computer to control communication with the computer system (Fig. 3 part 31); a transmit/receive control on the keyboard to control communication with the keyboard (Fig. 3 part 37); a main processor to create a secrete key, to perform secure mode setup/clearing according to the secure mode related commands, and to inter-transmit information of the computer system and the keyboard (Fig. 3 part 31); an initial cipher (column 5 line 61-62).

However Boebert does not disclose a cipher to encrypt the secret key from the main processor with a secure key from the computer system and then to transmit the encrypted secret key to the computer system, under secure mode; and a stream cipher to encrypt the key code input information with the secrete key from the main processor and then to transmit the encrypted information to the computer system, under secure mode.

Stallings disclose decentralized key distribution wherein transferring a secure key (Master key) to the Responder B. The Responder B creates a new secret key (session key) and uses the Master key to encrypt the session key and send it to the Initiator A (Page 147).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the key distribution as disclosed by Stallings between the cryptographic entity and the workstation of Boebert. One of ordinary skill in the art would have been motivated to do this because it would be a safe method of transferring a new session key whenever key codes need to be encrypted.

In reference to claim 4, further comprising a built-in secure mode indication lamp which is ON under secure mode, OFF under cleared secure: mode, and periodically blinks under disabled secure mode. The video display disclosed by Boebert performs the function of built-in secure mode indication lamp (column 5 lines 34-42).

In reference to claim 9, the decoding function uses the secret key is served by the keyboard manager of the computer system, or the operating system and/or application programs (Fig. 3).

In reference to claim 10, a protocol for acquiring decoded data exists between the keyboard manager and the application program, and between the keyboard manager and the application program (column 5 lines 55-65).

In reference to claim 11, further comprising the steps of main processor transferring the password from the transmit/receive control on the keyboard and the secure data from the transmit/receive control on the computer to the safe memory after the main processor transfers the password input request command to the computer system, and safe memory encrypting and then storing the received data using the password, if secure mode setup is made by the command from the application program of the computer system and also for data storage requiring security; but main processor transferring the password from the transmit/receive control on the keyboard to the safe memory after the main processor transfers the password input request command to the computer system, and safe memory decoding the encrypted data with the password and then transferring the decoded data to the main processor where the password is correct, but not decoding the encrypted data where not correct, if secure mode setup is made by the command from the application program of the computer system and also for acquisition of the secure data (column 6 lines 26-59).

In reference to claims 15-19, where a separate secure key for entering secure mode setup/clearing command is incorporated in said keyboard and/or the secure mode setup/clearing command can be created by the combination of existing key codes, the computer system has the secure key creation function, the encryption/decoding function with the secrete key and the encryption/decoding function with the secure key, and the keyboard manager with application program interface is included (column 5 line 66 to column 6 line 5).

Claims 5 and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boebert as applied to claims 1, 2, 3, and 4 above, and further in view of Stallings and Schneier.

Boebert discloses a cryptographic entity to decrypt data transmitted from the host to the display (column 5 lines 55-56), wherein the key must be a safe key and for the data to be display it must be saved in storage. Boebert also discloses an integrity mechanism (column 5 lines 56-58). Boebert's system further includes a comparison/processor to transmit the stored data to the decoder if two integrity identification values are the same after comparing the "password integrity identification value" received from the encryption/key operation processor with the "password integrity identification value" stored in the data storage memory, to transmit password nonconformity to the computer and delete the temporally stored safe key on the decoder if the values are not the same, and to transmit the data to the data storage memory where "encrypted data" and "encrypted data integrity identification value" together with "password integrity identification value" are received from the encryption/key operation processor. Since the system uses passwords to authenticate the trusted computing system, it is required to make a comparison between the password that it expects and the password that is received (column 6 lines 26-59). The system of Boebert also includes a data storage memory to store the encrypted data, the encrypted data integrity identification value and the password integrity identification value because these values are all used by the system and therefore would be stored by necessity.

However Boebert does not dislcose; converting the password to the key ("the safe key"), and then, if the secure data is not received together with the password from the safe memory interface, to transmit the safe key to the decoder and to encrypt the password with the safe key by encryption algorithm and calculate the integrity identification value of the encrypted password ("password integrity identification value") and then to transmit the password integrity identification value to a comparison/processor, and, if the secure data is received together with the password from the safe memory interface, to encrypt the secure data with the safe key and calculate the Integrity identification value of the encrypted secure data ("encrypted data integrity identification value") and then to transmit the encrypted data integrity identification value together with the "encrypted data" to the comparison/processor; a comparison/processor to transmit the stored data to the decoder if two integrity identification values are the same after comparing the "password integrity identification value" received from the encryption/key operation processor with the "password integrity identification value" stored in the data storage memory, to transmit password nonconformity to the computer and delete the temporally stored safe key on the decoder if the values are not the same, and to transmit the data to the data storage memory where "encrypted data" and "encrypted data integrity identification value" together with "password integrity identification value" are received from the encryption/key operation processor; a data storage memory to store the encrypted data, the encrypted data integrity identification value and the password integrity identification value;

Stallings disclose decentralized key distribution wherein transferring a secure key (Master key) to the Responder B. The Responder B creates a new secret key (session key) and uses the Master key to encrypt the session key and send it to the Initiator A (Page 147). The session key performs the function of a password to authenticate the user because if the user does not have the correct Master key and therefore is not authentic then the session key will be decrypted incorrectly. The nonce is the secure data that is sent with the session key.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the key distribution as disclosed by Stallings between the cryptographic entity and the workstation of Boebert. One of ordinary skill in the art would have been motivated to do this because it would be a safe method of transferring a new session key whenever key codes need to be encrypted.

Schneier discloses a process of converting a password to a key using a hash function (pages 174-175). The hash of the pass phrase can be sent with the messages as shown in the algorithm for digital signatures (page 41 section 2.7) since the digital signature algorithm also calculates the hash value of the message.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the hash of the pass phrase (password) and send it with the message (secure data) as in Schneier in the system of Beobert. One of ordinary skill in the art would have been motivated to do this because the receiver can be confident that the data has not been changed and was received from the correct sender.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Boebert, Stallings, and Schneier as applied to claim 5 above, and further in view of Ramabadran

Boebert, Stallings, and Schneier do not expressly disclose a system where, the said integrity identification value is calculated using the CRC algorithm.

Ramabadran discloses calculating the CRC for preserving the integrity of data in storage and transmission (Introduction).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the CRC to preserve the integrity of the transmitted data as in Ramabadran in the system of Beobert. One of ordinary skill in the art would have been motivated to do this because it would increase the confidence that the password information and secure data were on changed while still on transit.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

The 2100 Tech center will move to Carlyle in October 2004. The new telephone number for the receptionist is (571) 272-2100. The examiner's new telephone number will be (571) 272-3854.

PATENT EX
Y CENTER 2